

FIG. 1

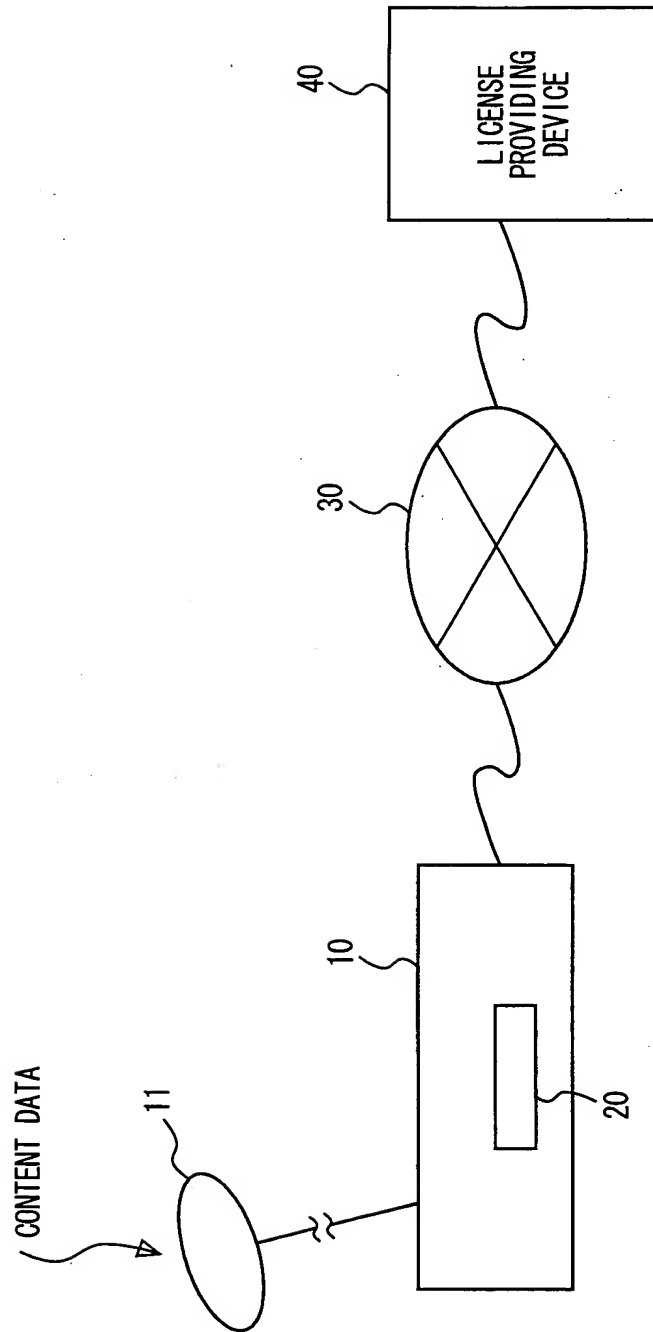


FIG. 2

SYMBOL	NAME	ATTRIBUTE	CHARACTERISTICS
Dc	DATA	PECULIAR TO DATA	EX.: MUSIC, READING, EDUCATIONAL OR IMAGE DATA, RECORDED AND MANAGED AS ENCRYPTED CONTENT DATA E(Kc, Dc) ENCRYPTED WITH Kc
Di	DATA INFORMATION	PECULIAR TO DATA	PLAINTEXT DATA RELATED TO Dc AND INCLUDING DID
DID	DATA ID	PECULIAR TO DATA	MANAGEMENT CODE FOR SPECIFYING Dc AND Kc
Kc	CONTENT KEY	PECULIAR TO DATA	SYMMETRIC KEY ENCRYPTING/DECRYPTING ENCRYPTED DATA
AC	CONTROL INFORMATION	PECULIAR TO LICENSE	RESTRICTIONS RELATED TO REPRODUCTION AND LICENSE HANDLING
LID	LICENSE ID	PECULIAR TO LICENSE	MANAGEMENT CODE FOR SPECIFYING LICENSE
LIC	LICENSE	PECULIAR TO LICENSE	GENERALLY REPRESENTING Kc//AC//DID//LID

FIG. 3

	SYMBOL	NAME	CHARACTERISTIC
LICENSE PROVIDING DEVICE	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED FOR EVERY LICENSE DISTRIBUTION SYMMETRIC KEY
	Ka	MASTER KEY	PRIVATE ENCRYPTION KEY TO BE USED FOR PRODUCING CLASS CERTIFICATE OPERATED BY CERTIFICATION AUTHORITY
DATA STORAGE DEVICE (HARD DISK)	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	KPomy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
	Komy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPomy
	Iomy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Gmy	CLASS CERTIFICATE	$Gmy = KPomy // Iomy // E(Ka, H(KPomy // Iomy))$ CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	KPomz	INDIVIDUAL PUBLIC KEY	INDIVIDUAL PUBLIC ENCRYPTION KEY HAVING VALUE PECULIAR TO EACH DATA STORAGE DEVICE "z" IS IDENTIFIER IDENTIFYING DATA STORAGE DEVICE
	Komz	INDIVIDUAL PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH INDIVIDUAL PUBLIC KEY KPomz
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE PROVIDER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
	KPcpy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
REPRODUCING CIRCUIT	Kcpy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPcpy
	Icpy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Gpy	CLASS CERTIFICATE	$Gpy = KPcpy // Icpy // E(Ka, H(KPcpy // Icpy))$ CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY

FIG. 4

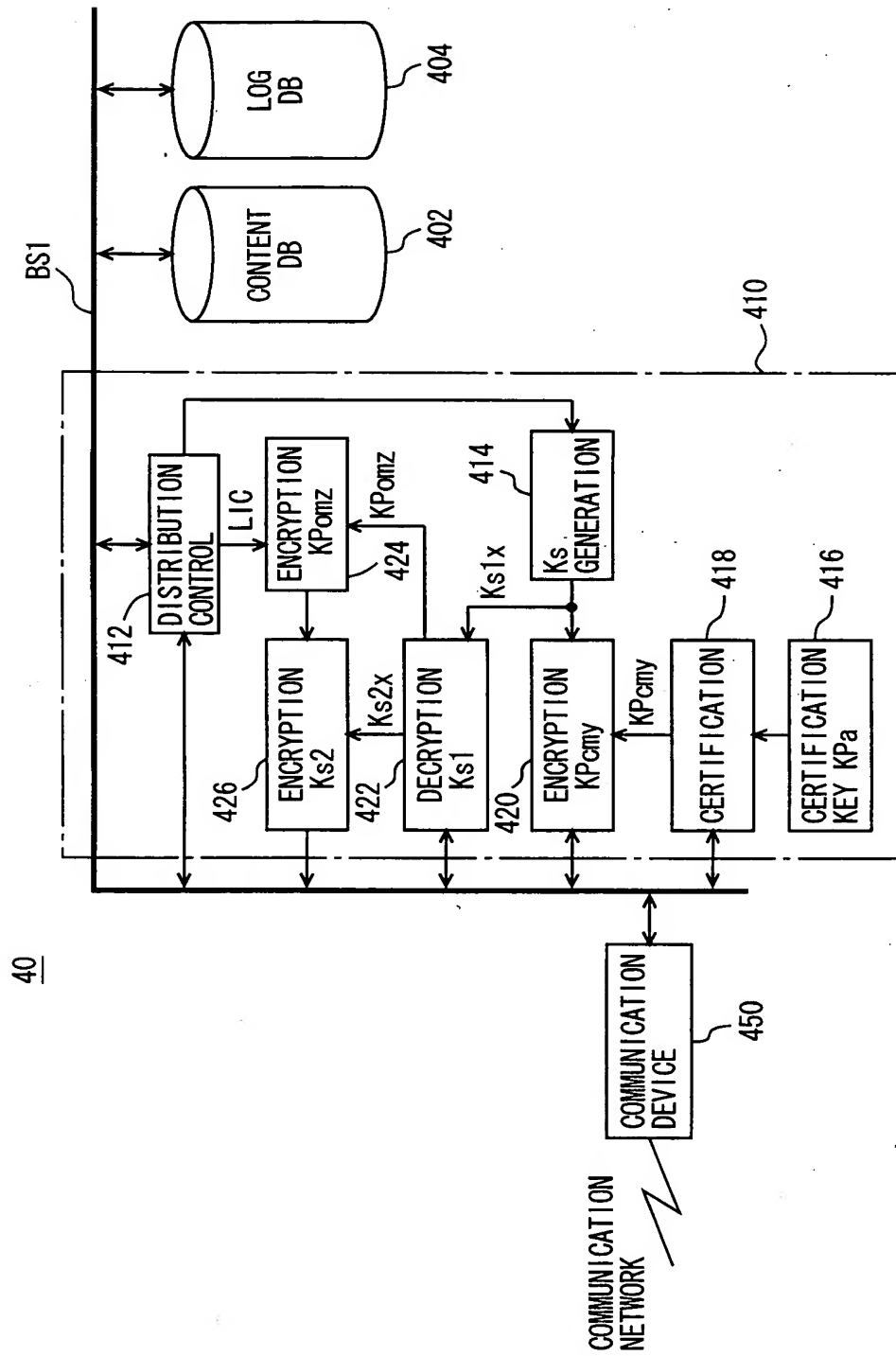


FIG. 5

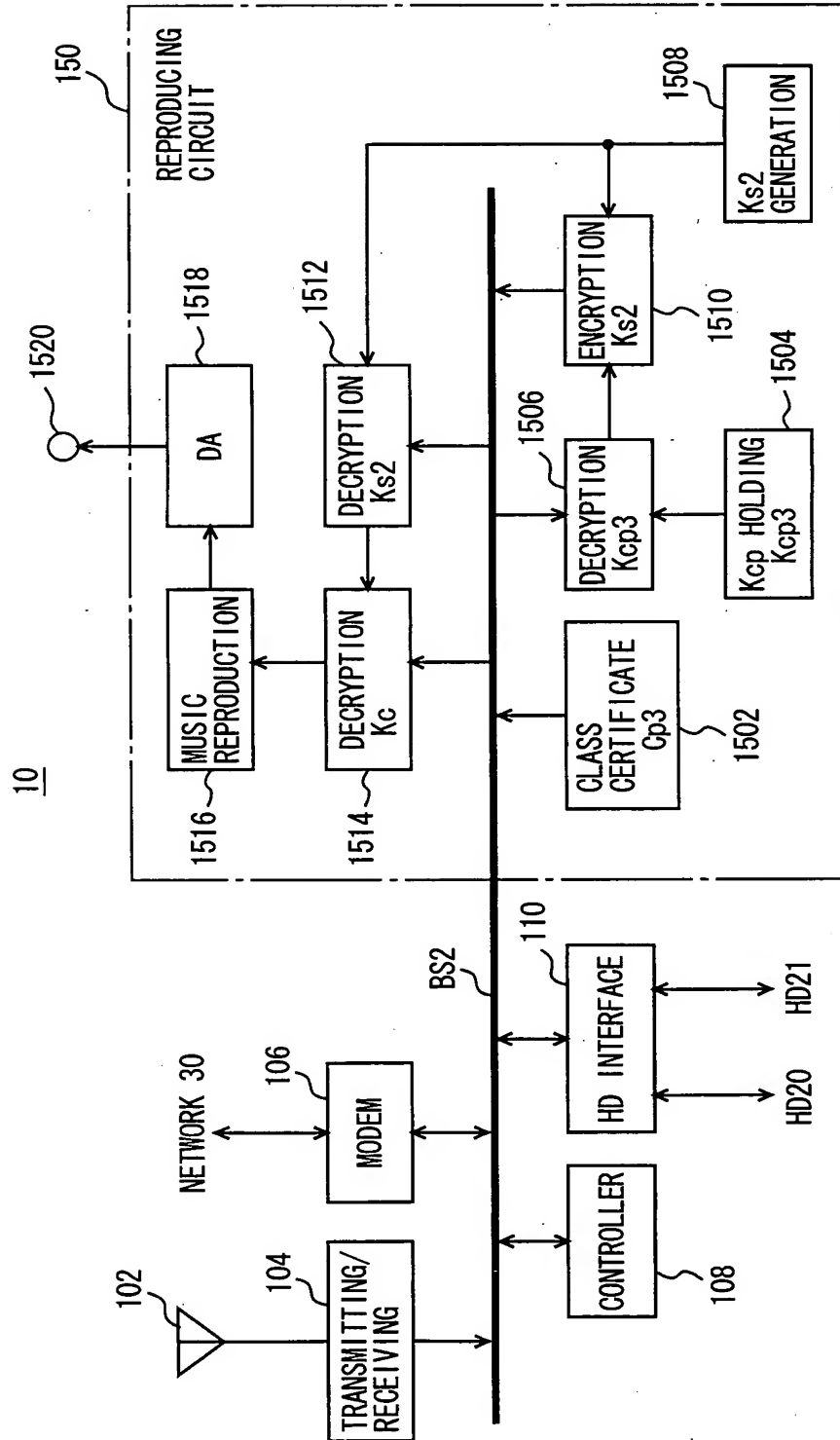


FIG. 6

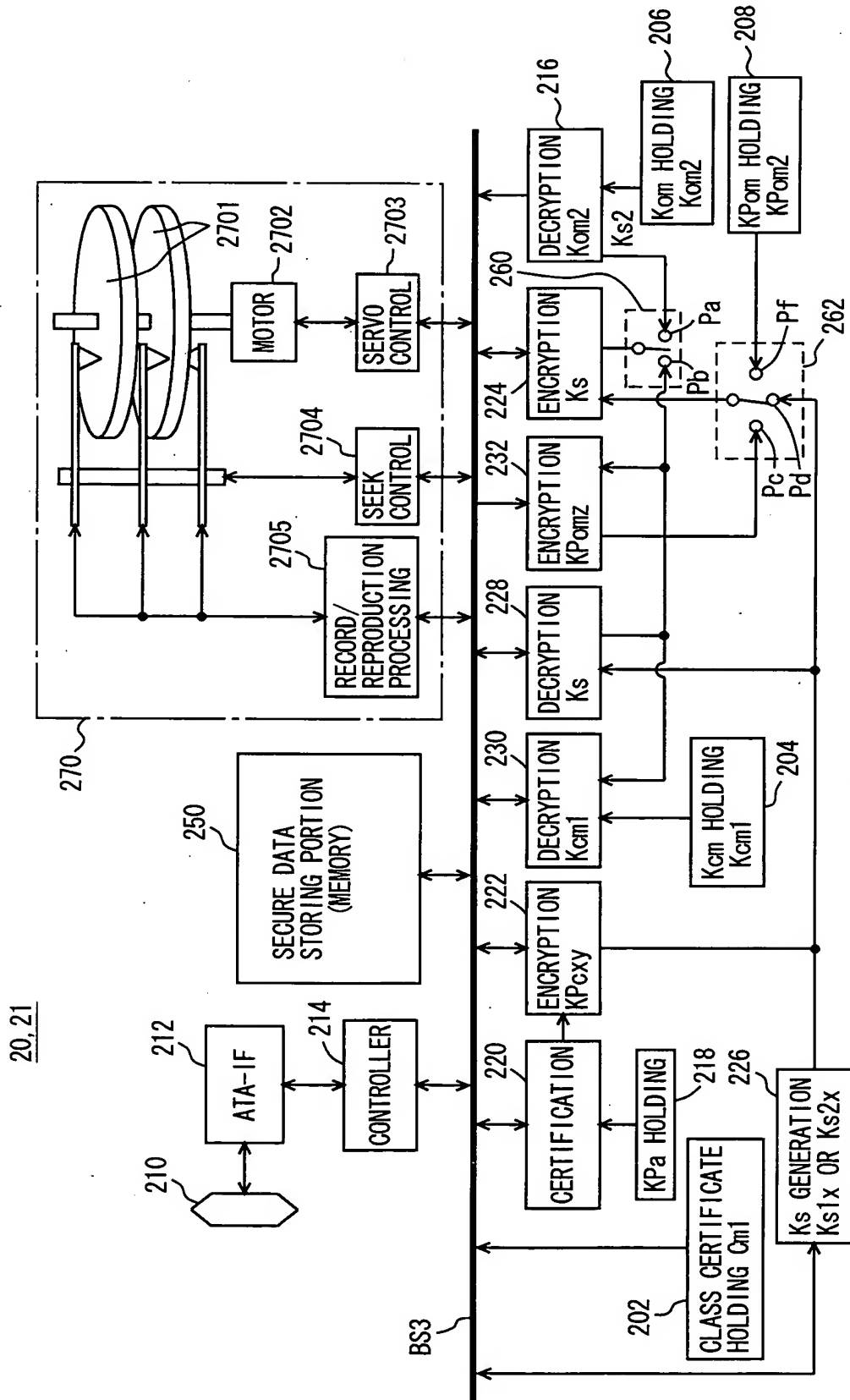


FIG. 7

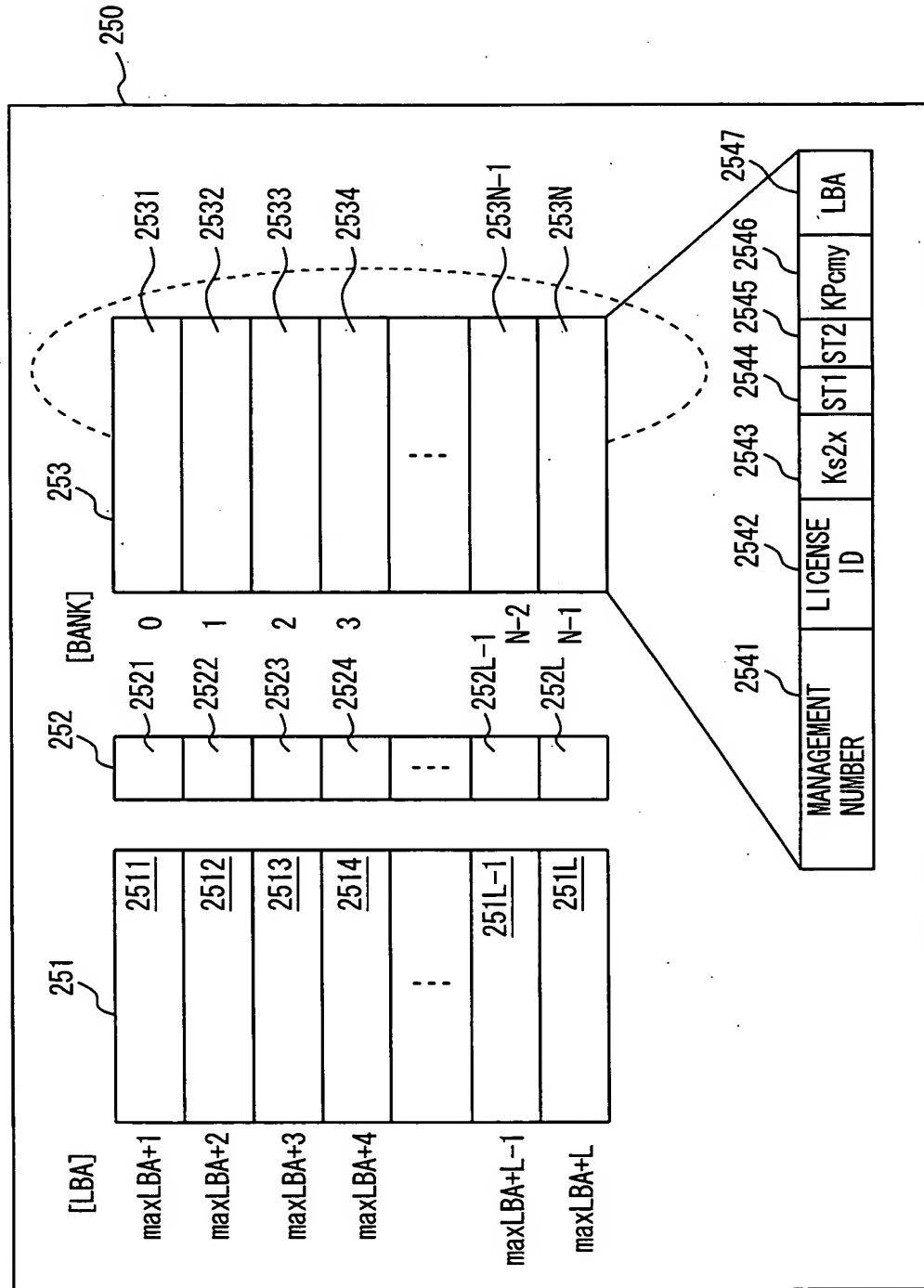


FIG. 8

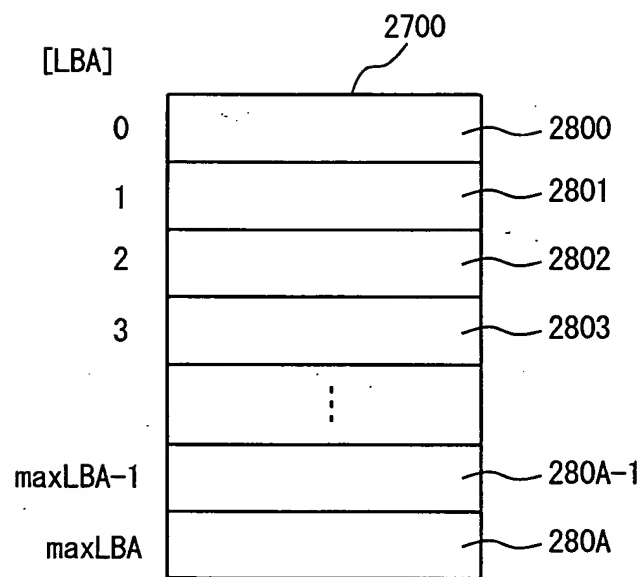




FIG. 9

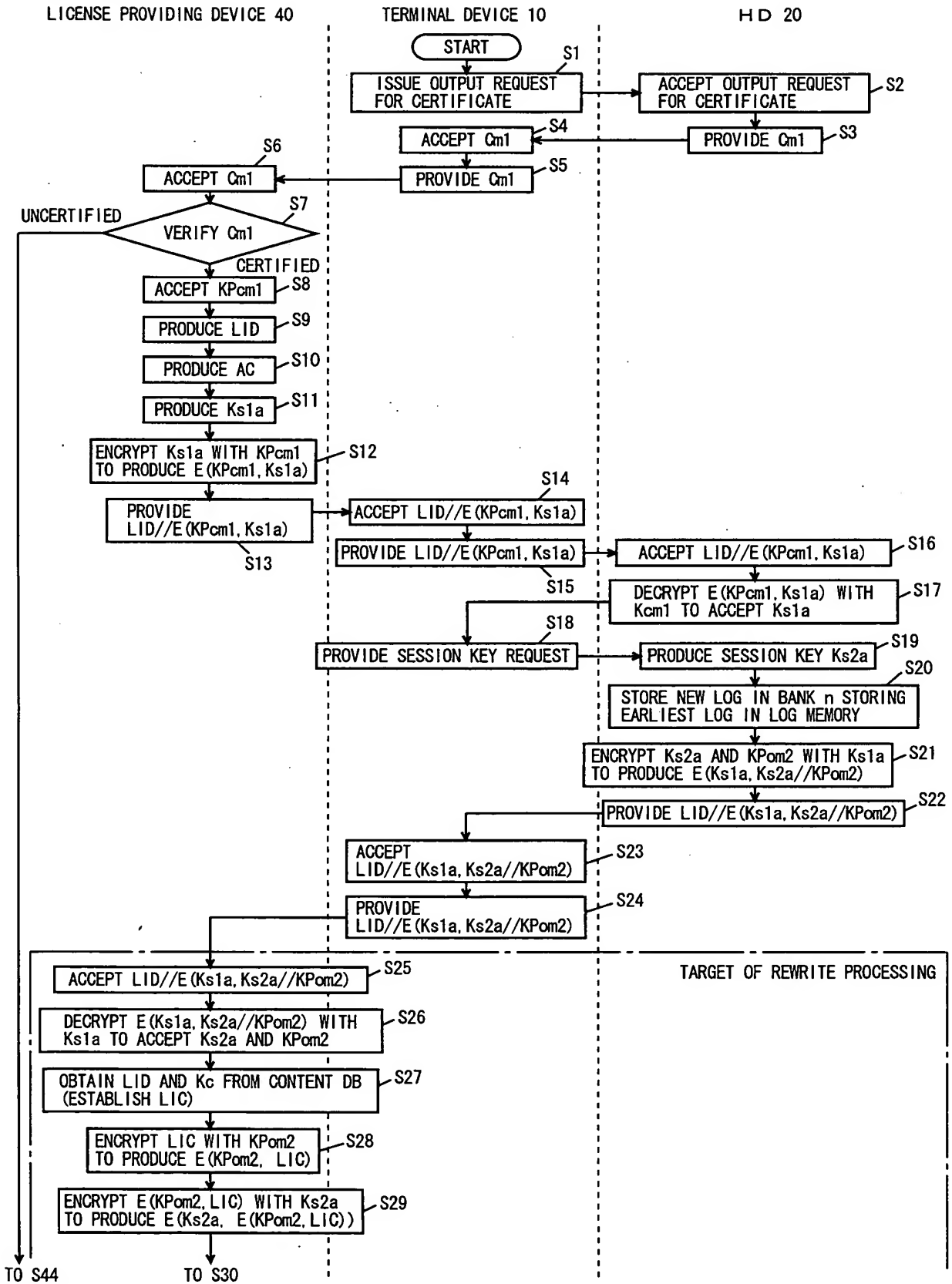


FIG. 10

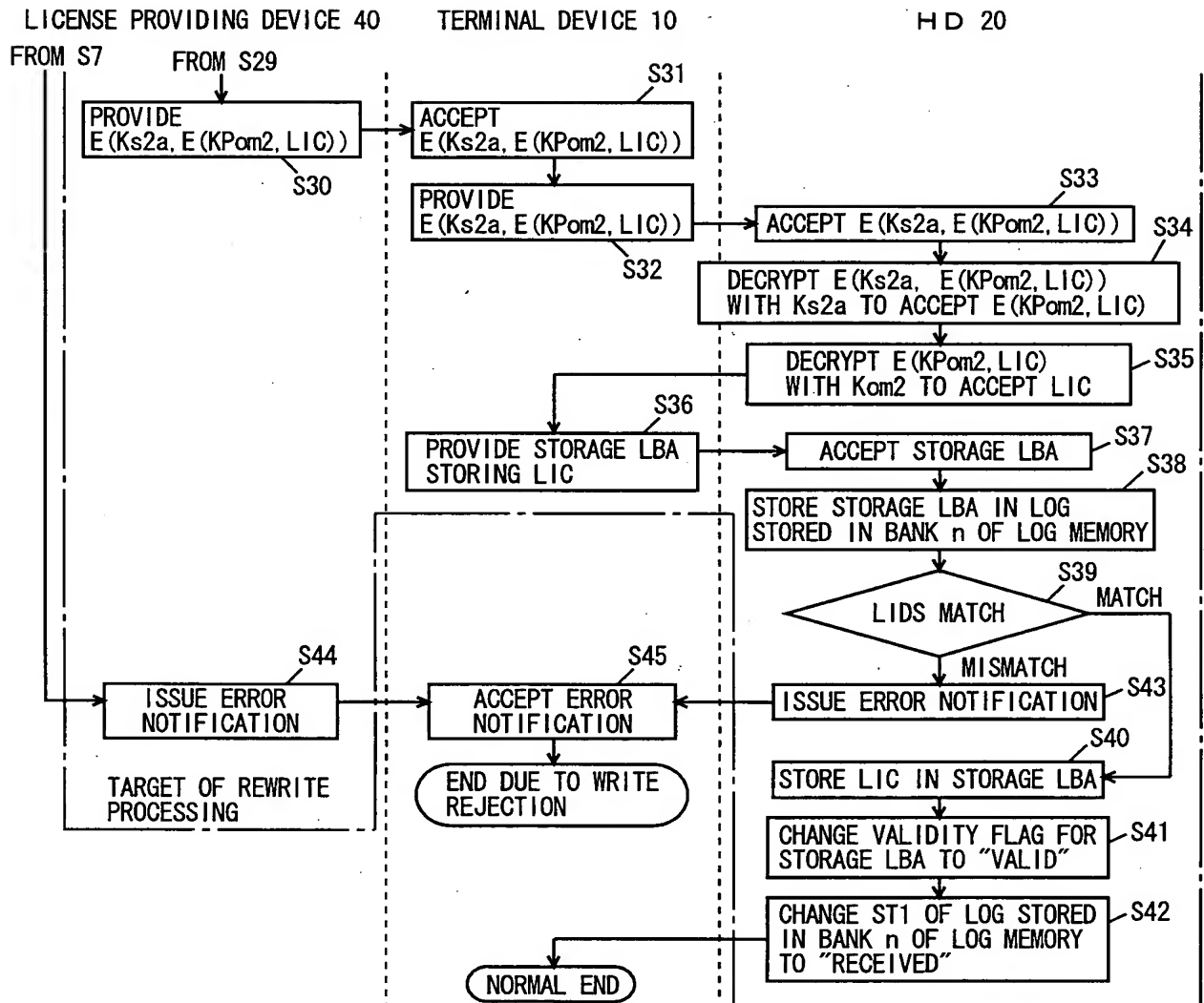


FIG. 11

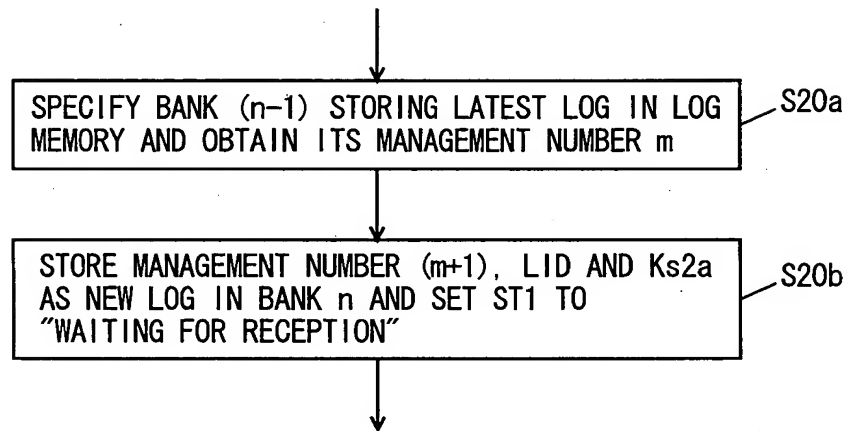


FIG. 12

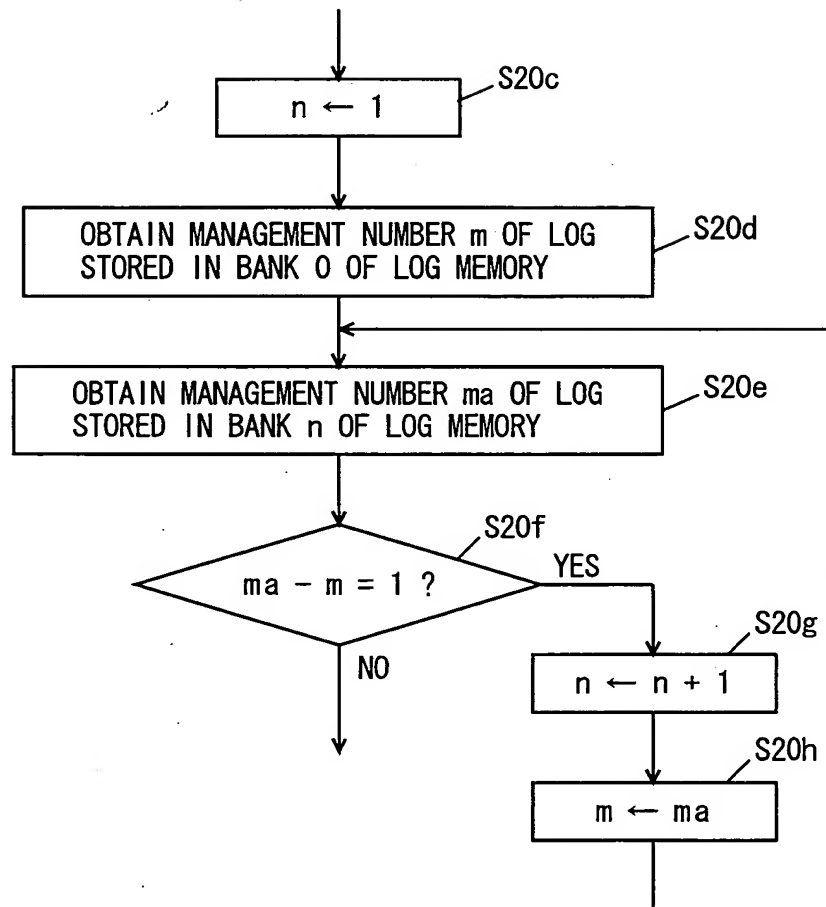


FIG. 13

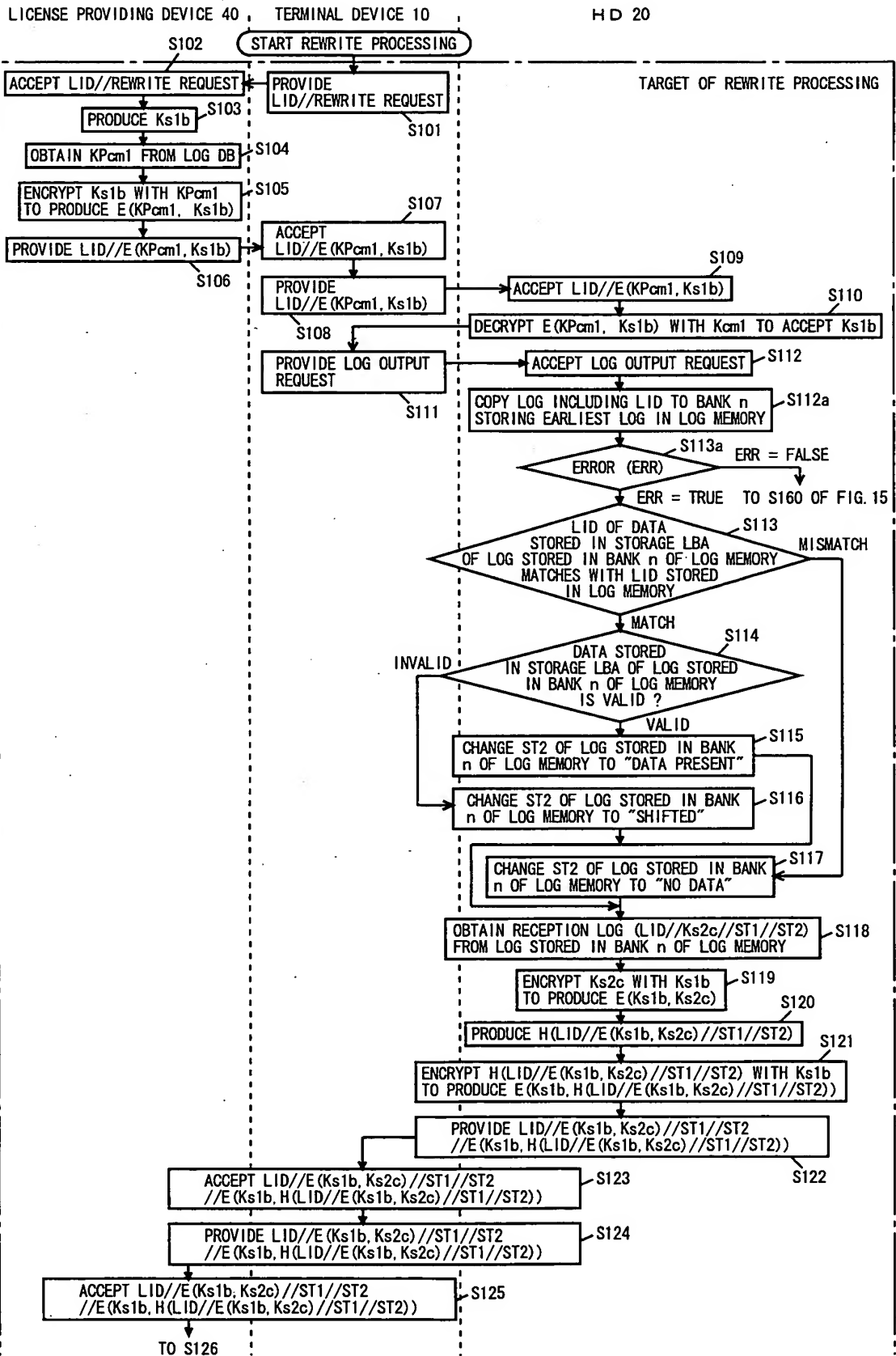


FIG. 14

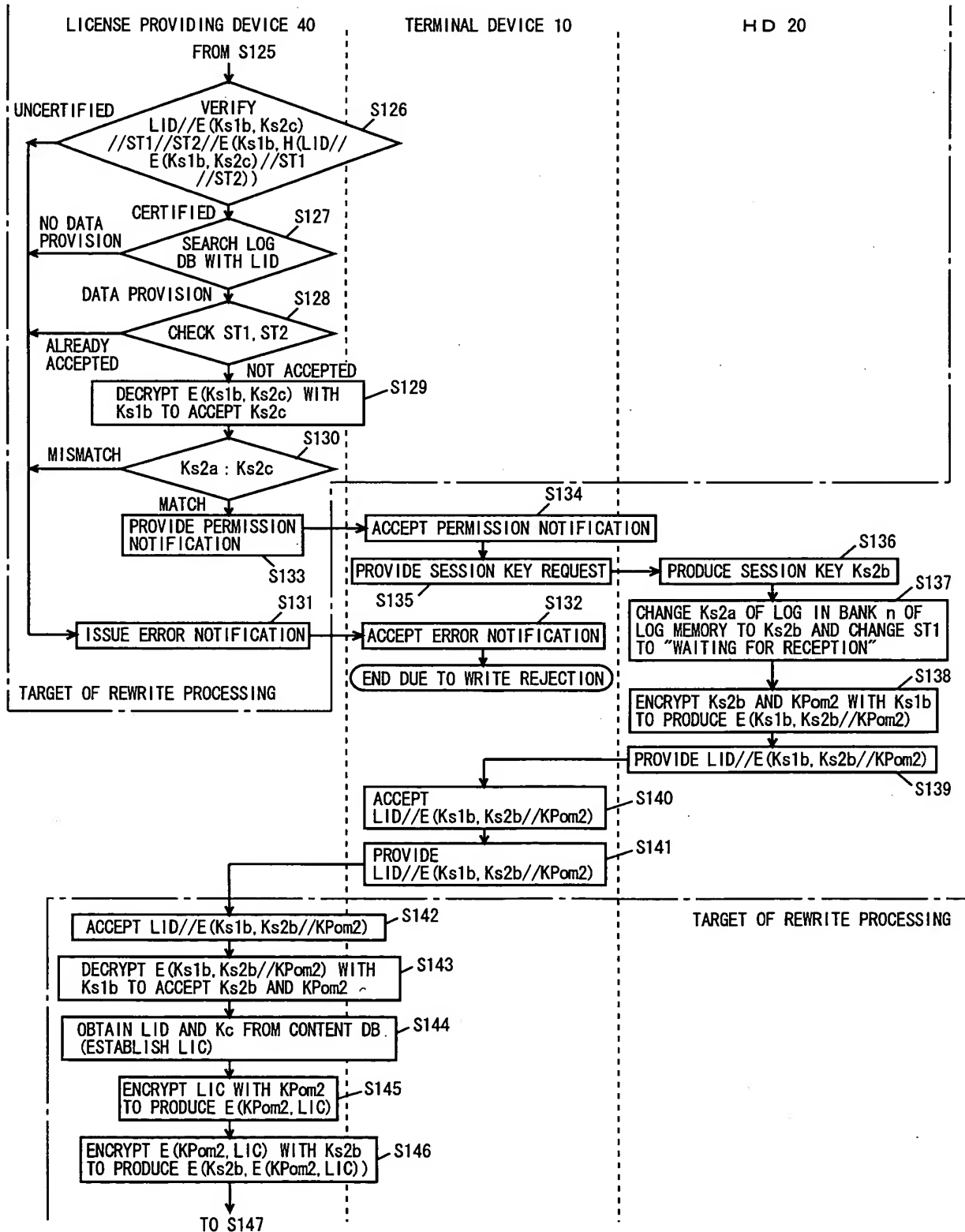


FIG. 15

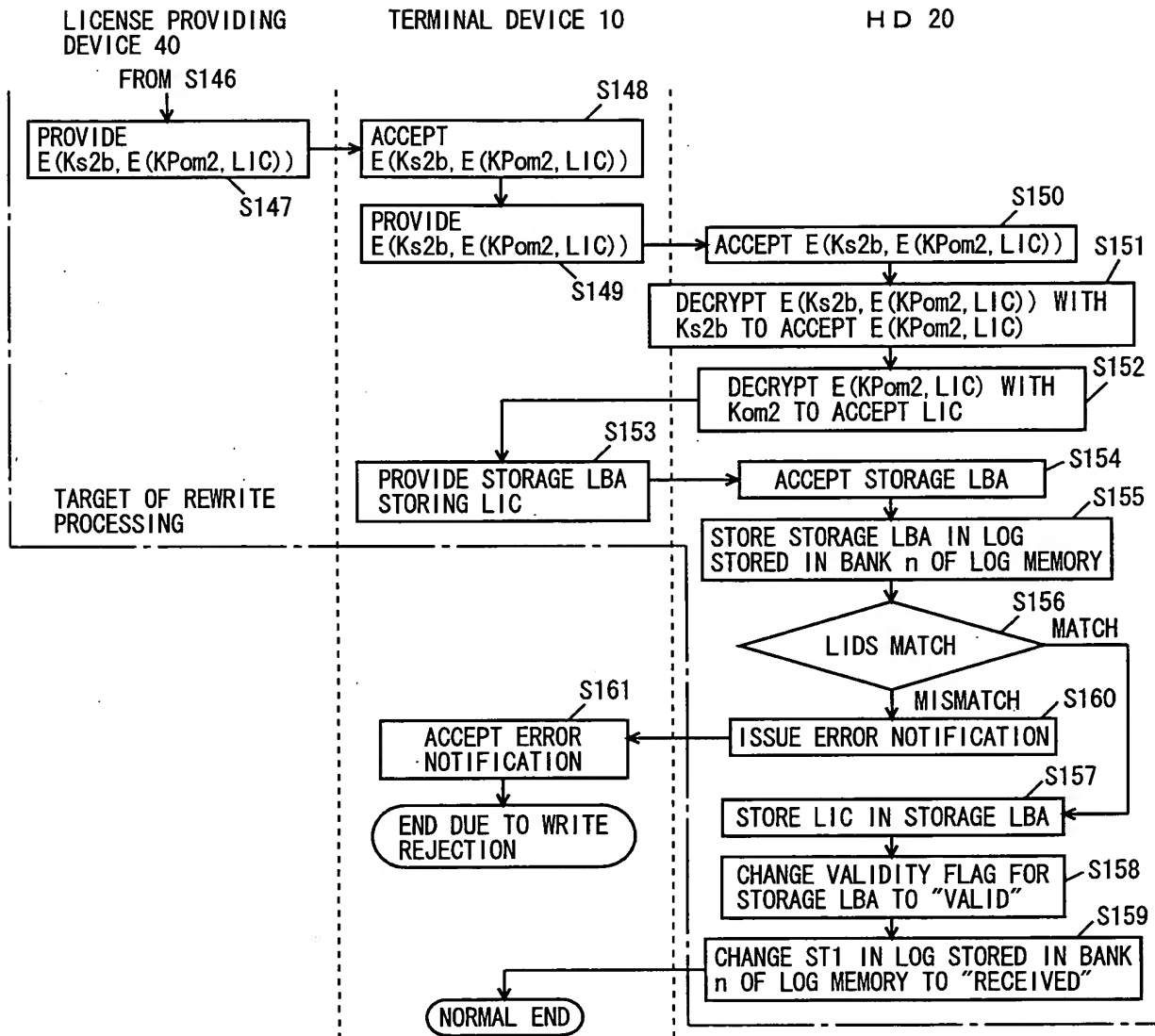


FIG. 16

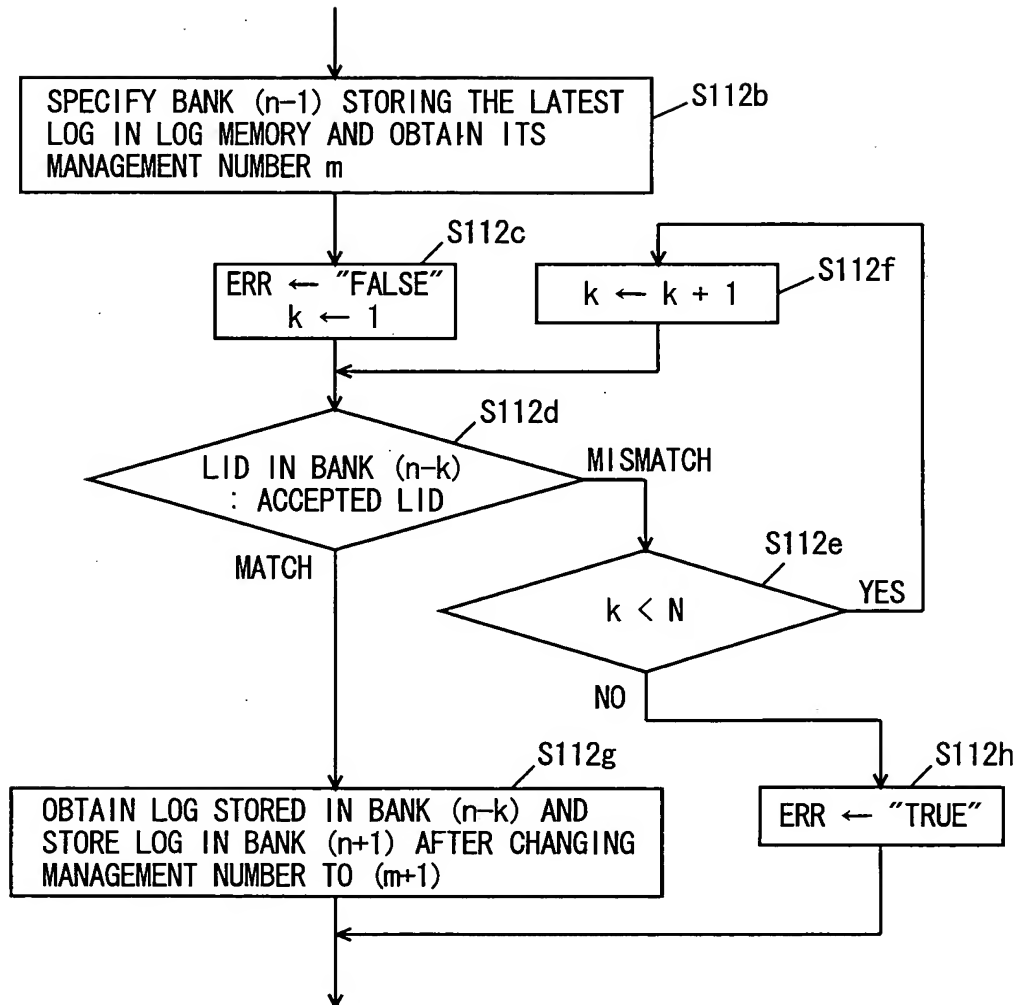
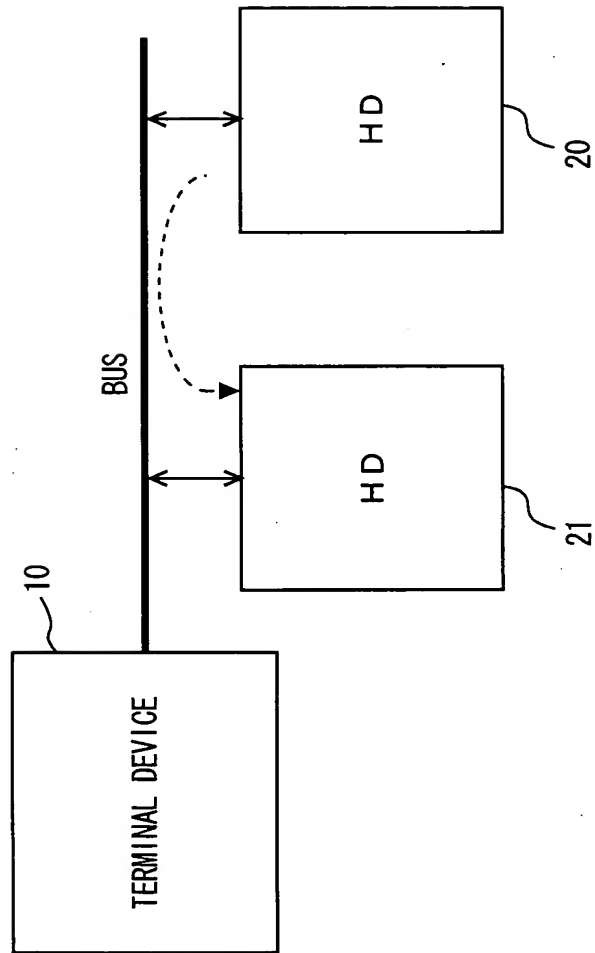


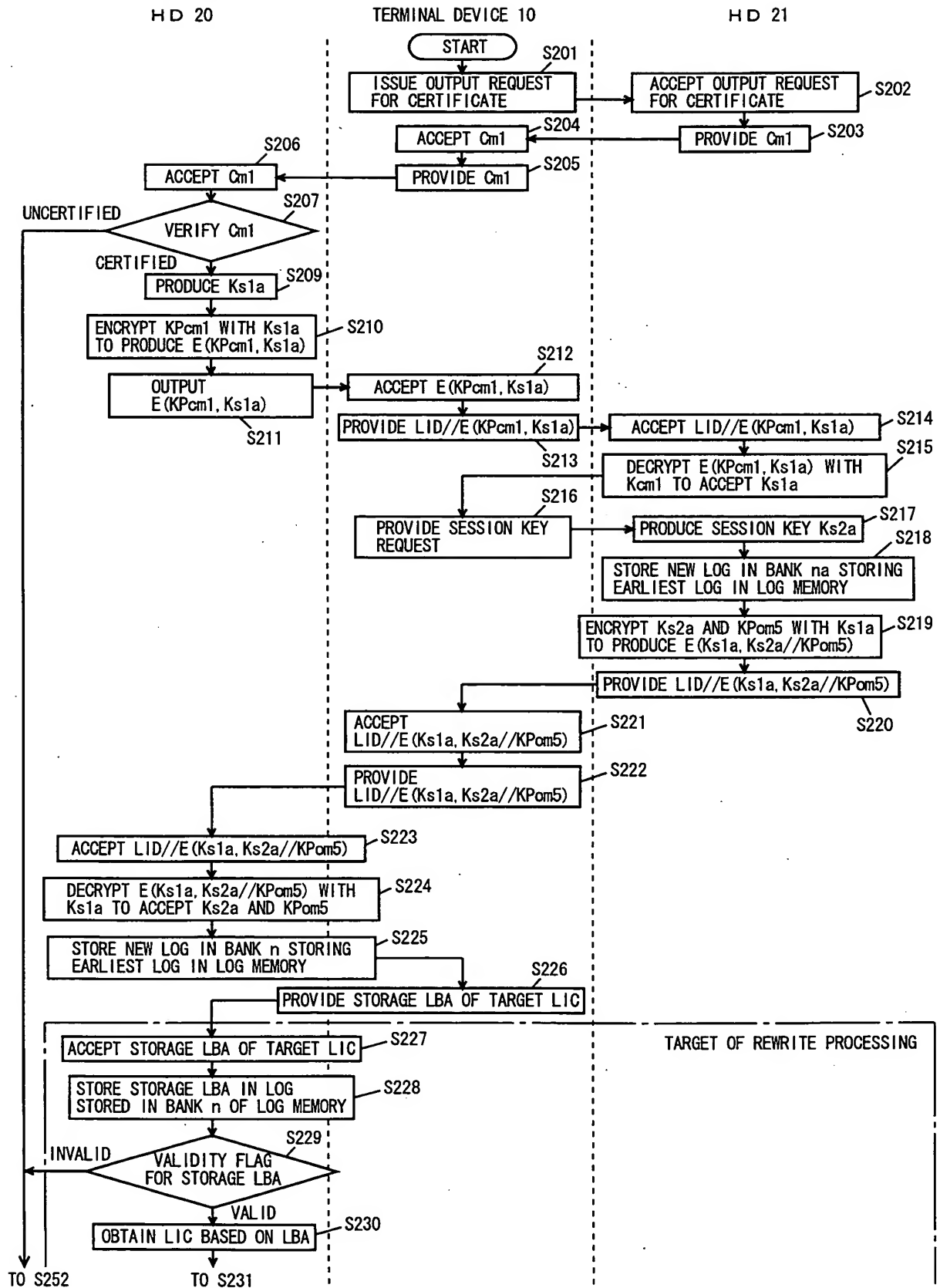


FIG. 17



Rec'd PET/PTO 24 JAN 2005

FIG. 18



Rec'd PGT/PTO 24 JAN 2005

FIG. 19

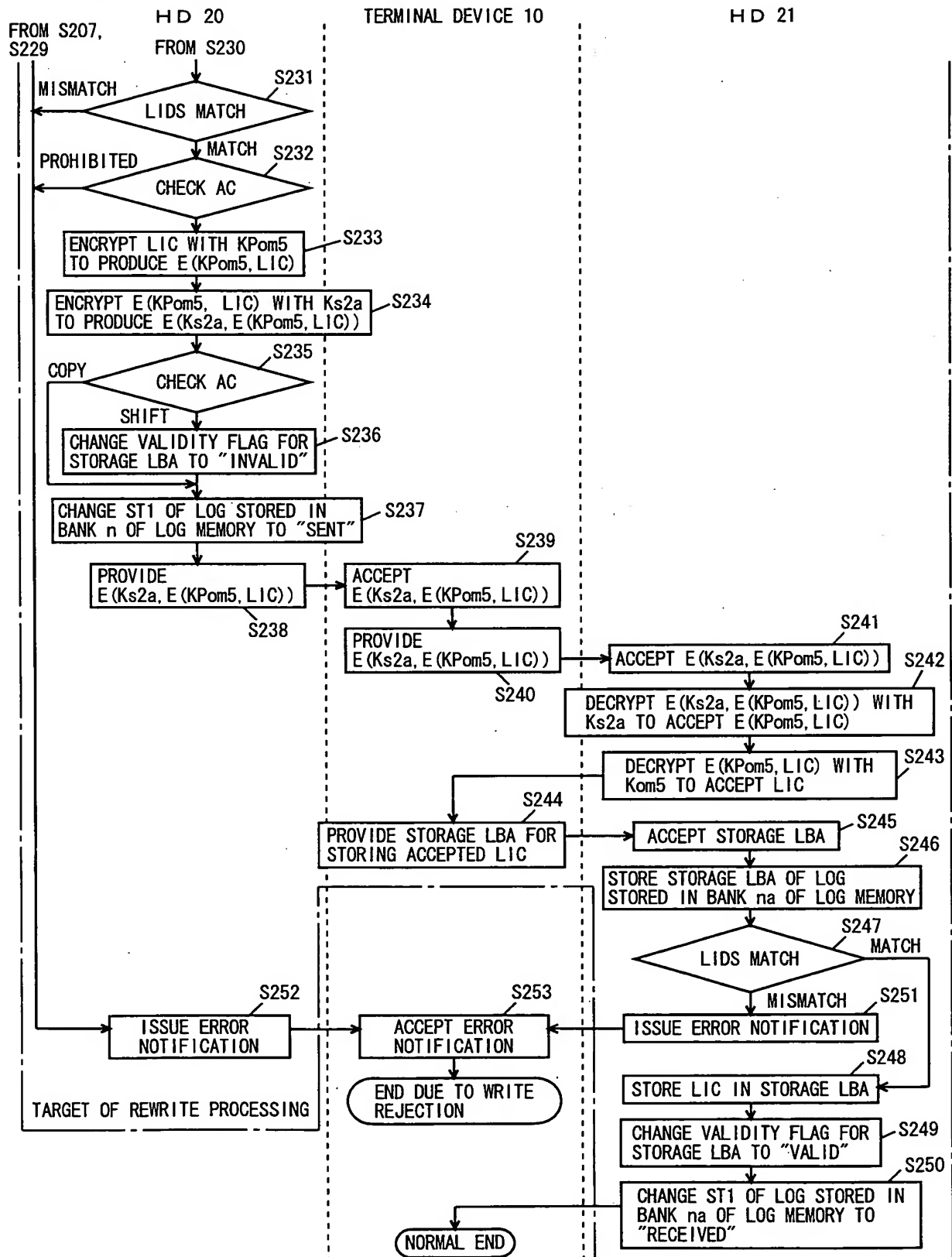
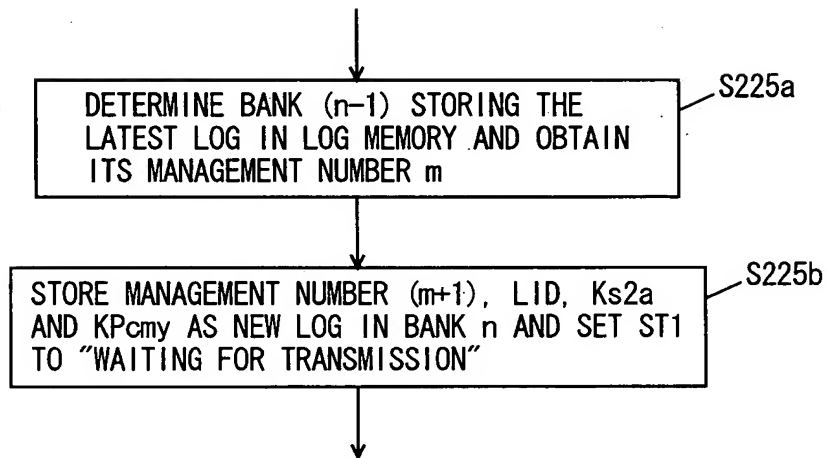
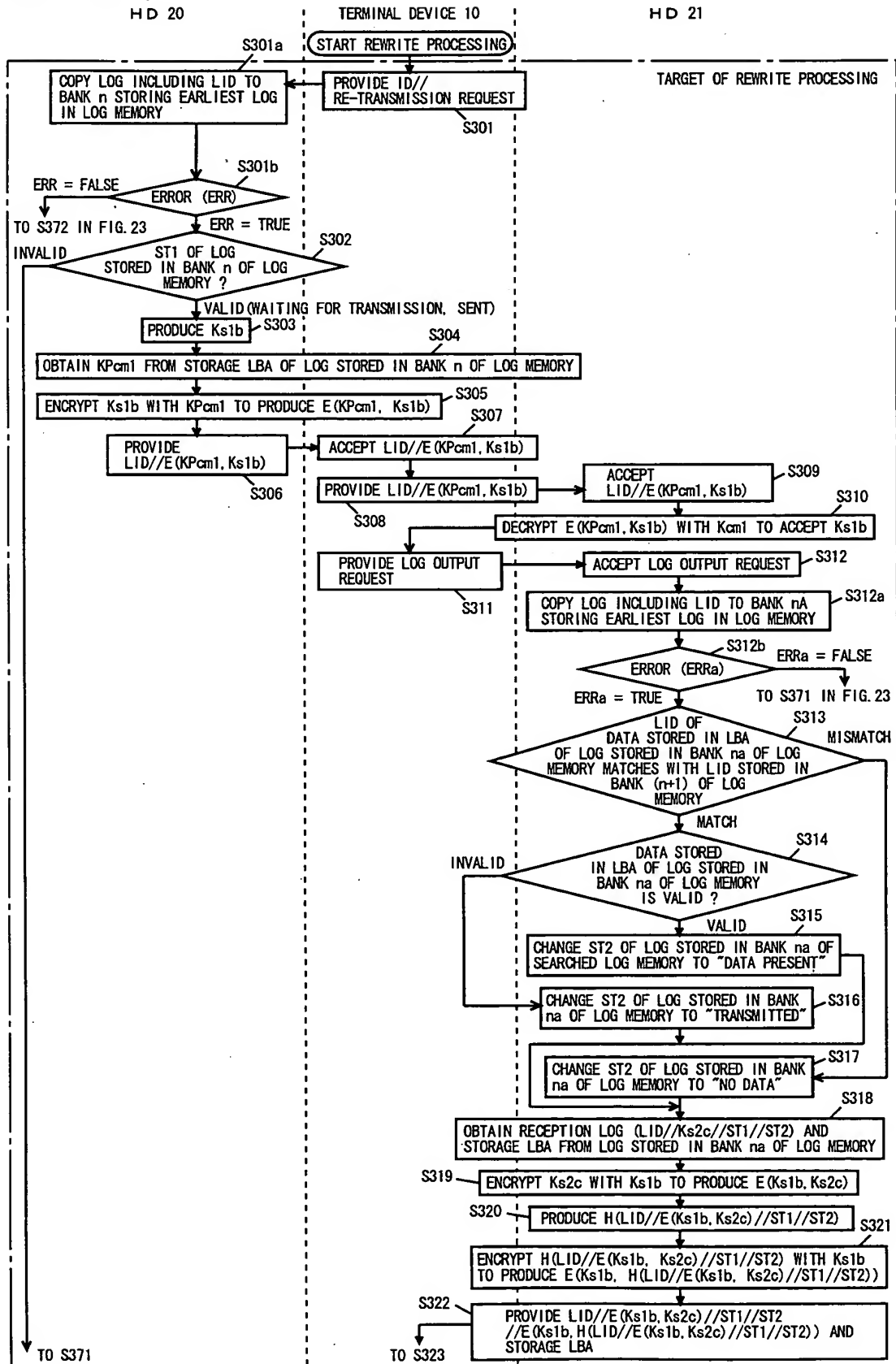


FIG. 20



Rec'd PET/PTO 24 JAN 2005

FIG. 21



```

graph TD
    subgraph FROM_S302 [FROM S302]
        S325[ACCEPT LID//E(Ks1b, Ks2c)//ST1//ST2  
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))]
        S326{VERIFY  
LID//E(Ks1b, Ks2c)  
//ST1//ST2//E(Ks1b, H(LID//  
E(Ks1b, Ks2c)//ST1  
//ST2))}
        S327{CHECK LID}
        S328[DECRYPT E(Ks1b, Ks2c) WITH  
Ks1b TO ACCEPT Ks2c]
        S329{Ks2a : Ks2c}
        S330{CHECK  
RECEIVED ST1,  
ST2}
        S331{LID OF DATA  
STORED IN STORAGE  
LBA OF LOG STORED IN BANK n  
OF LOG MEMORY MATCHES WITH  
LID STORED IN LOG  
MEMORY ?}
        S332{VALIDITY  
FLAG FOR STORAGE LBA  
OF LOG STORED IN BANK n  
OF LOG MEMORY}
        S333[VALIDATE SEARCHED LICENSE]
        S334[PROVIDE STORAGE LBA OF LOG  
STORED IN BANK n OF LOG MEMORY  
AND USAGE PERMISSION]
        S335[ACCEPT STORAGE LBA  
AND USAGE PERMISSION]
        S336[PROVIDE SESSION KEY  
REQUEST]
        S337[PRODUCE SESSION KEY Ks2b]
        S338[CHANGE Ks2a OF LOG IN BANK na OF LOG MEMORY TO  
Ks2b AND CHANGE ST1 TO "WAITING FOR RECEPTION"]
        S339[ENCRYPT Ks2b AND KPom5 WITH Ks1b  
TO PRODUCE E(Ks1b, Ks2b//KPom5)]
        S340[PROVIDE LID//E(Ks1b, Ks2b//KPom5)]
        S341[ACCEPT  
LID//E(Ks1b, Ks2b//KPom5)]
        S342[PROVIDE  
LID//E(Ks1b, Ks2b//KPom5)]
        S343[ACCEPT LID//E(Ks1b, Ks2b//KPom5)]
        S344[DECRYPT E(Ks1b, Ks2b//KPom5) WITH  
Ks1b TO ACCEPT Ks2b AND KPom5]
    end

    subgraph FROM_S322 [FROM S322]
        S323[ACCEPT LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b,  
Ks2c)//ST1//ST2)) AND STORAGE LBA]
        S324[PROVIDE LID//E(Ks1b, Ks2c)//ST1//ST2  
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))]
    end

    subgraph HD_21 [HD 21]
        S335 --> S336
        S336 --> S337
        S337 --> S338
        S338 --> S339
        S339 --> S340
        S340 --> S341
        S341 --> S342
        S342 --> S343
        S343 --> S344
    end

    S323 --> S324
    S324 --> S325
    S325 --> S326
    S326 -- UNCERTIFIED --> S326
    S326 -- CERTIFIED --> S327
    S327 -- MISMATCH --> S326
    S327 -- MATCH --> S328
    S328 --> S329
    S329 -- MISMATCH --> S326
    S329 -- MATCH --> S330
    S330 -- ALREADY ACCEPTED --> S326
    S330 -- NOT ACCEPTED --> S331
    S331 -- MISMATCH --> S326
    S331 -- MATCH --> S332
    S332 -- VALID --> S333
    S332 -- INVALID --> S333
    S333 --> S334
    S334 --> S335
    S335 --> S336
    S336 --> S337
    S337 --> S338
    S338 --> S339
    S339 --> S340
    S340 --> S341
    S341 --> S342
    S342 --> S343
    S343 --> S344
    S344 --> S371[TO S371]
    S345[TO S345]

```

Rec'd PET/PTO 24 JAN 2005

FIG. 23

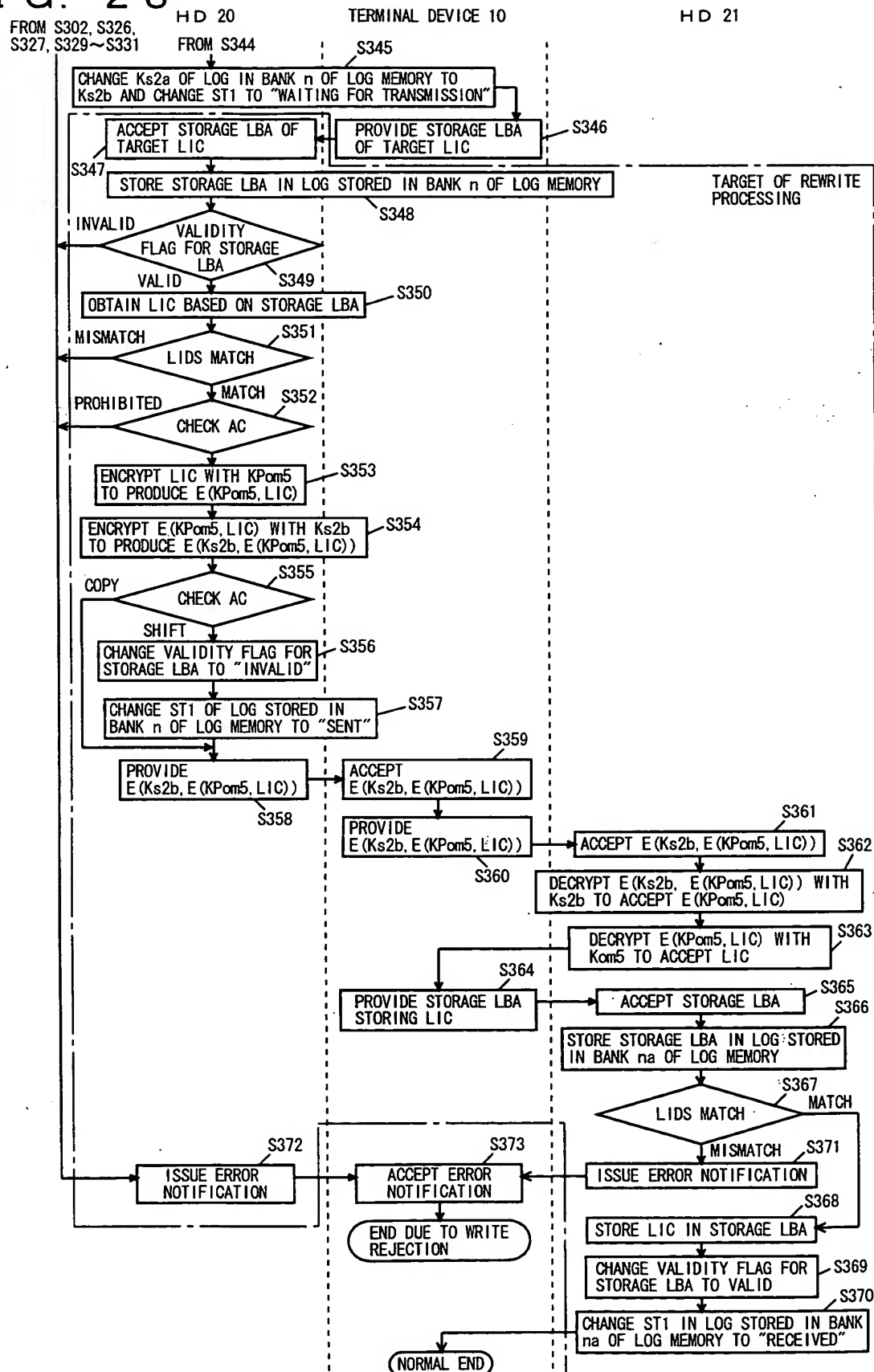


FIG. 24

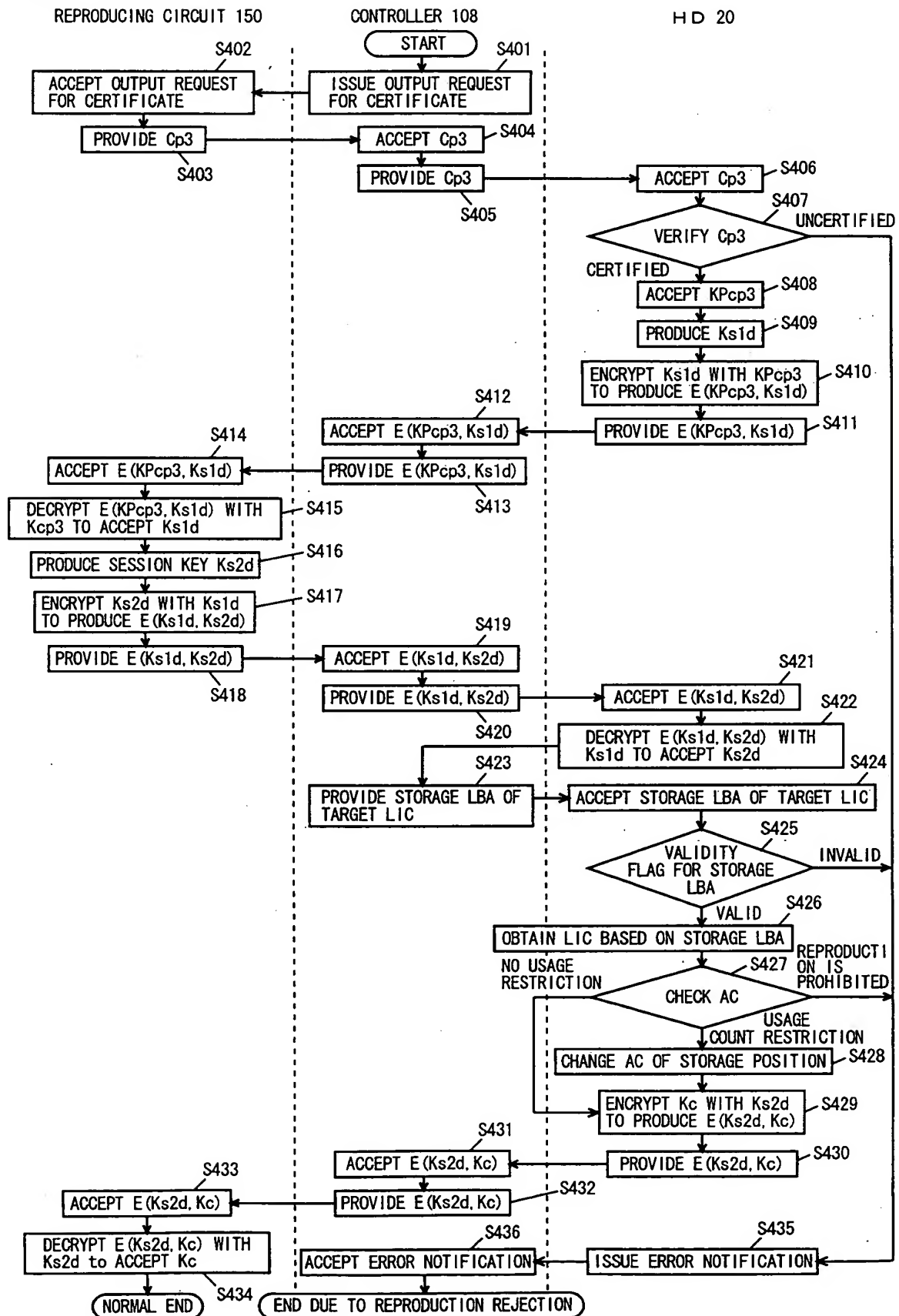




FIG. 25

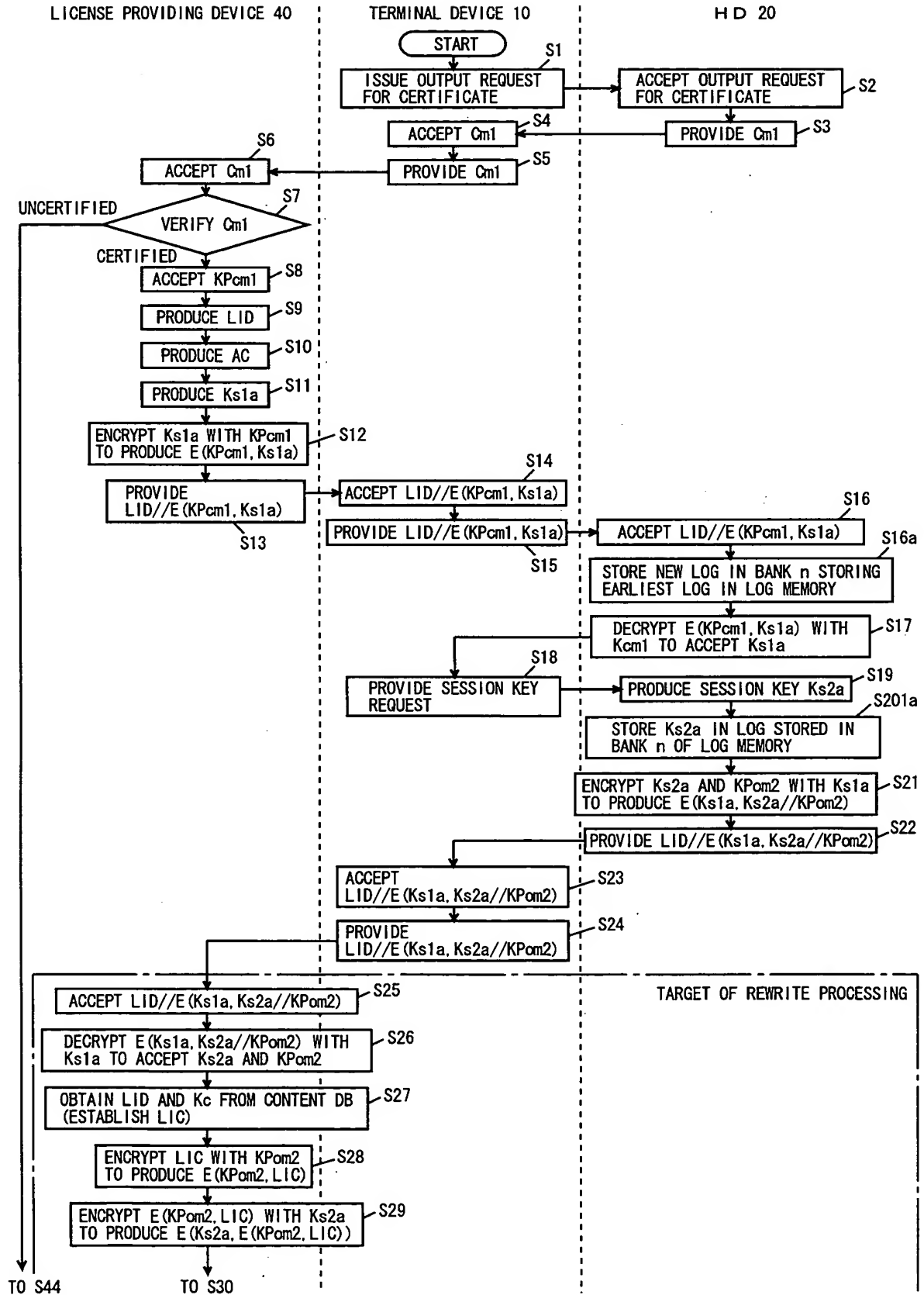


FIG. 26

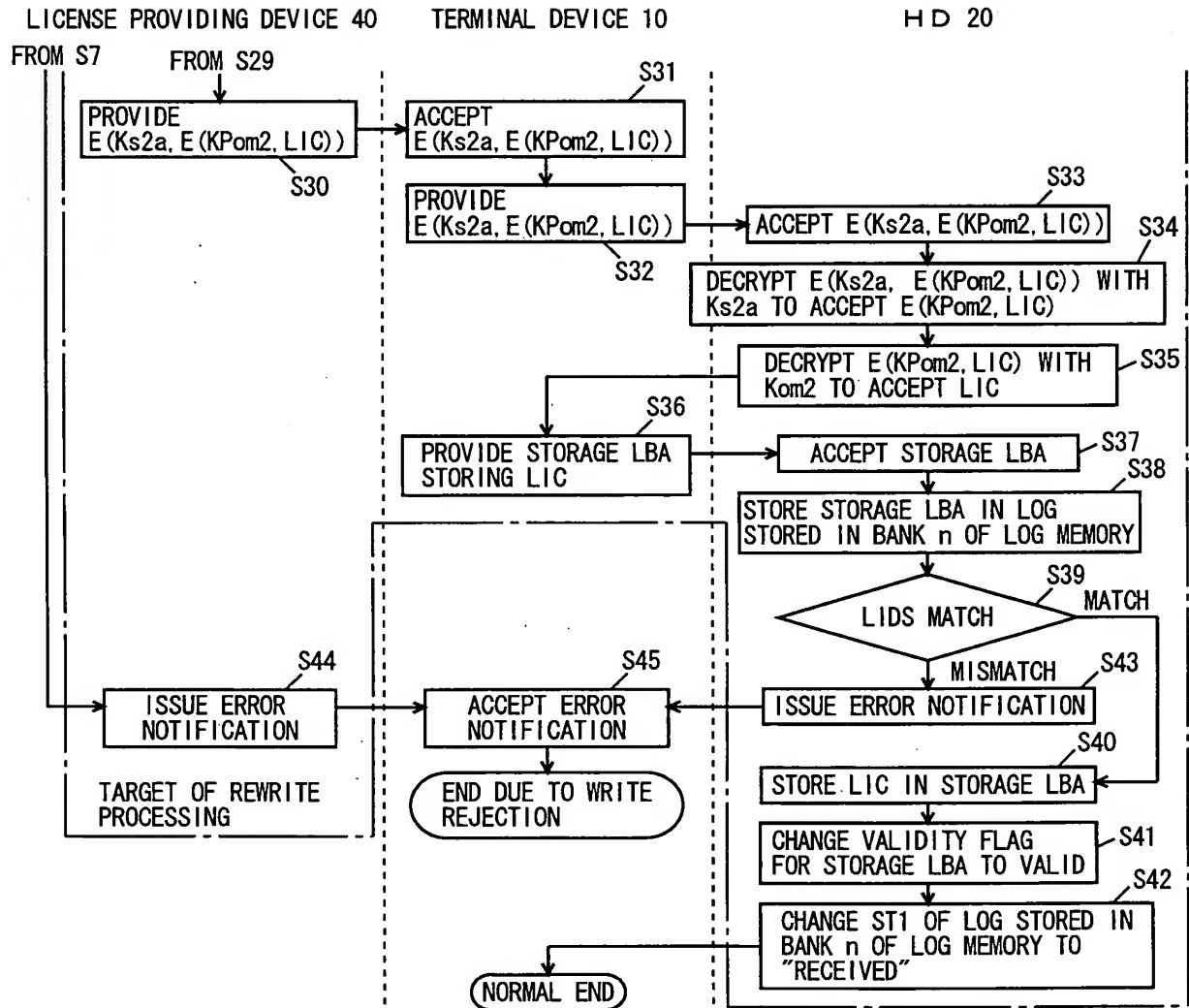
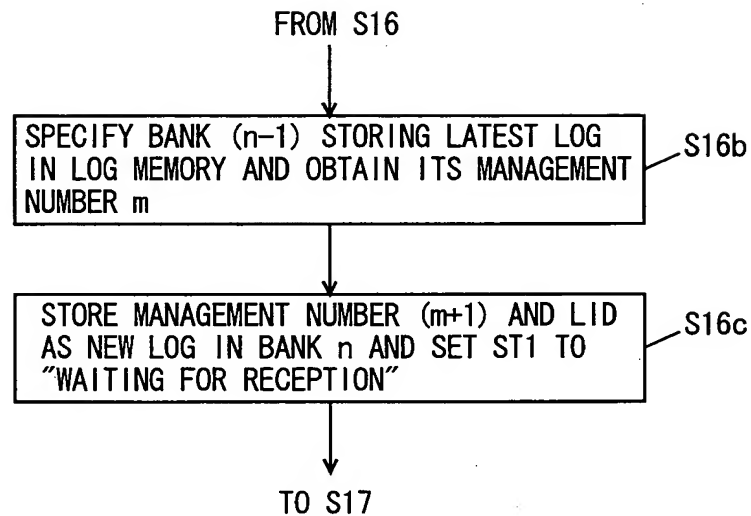
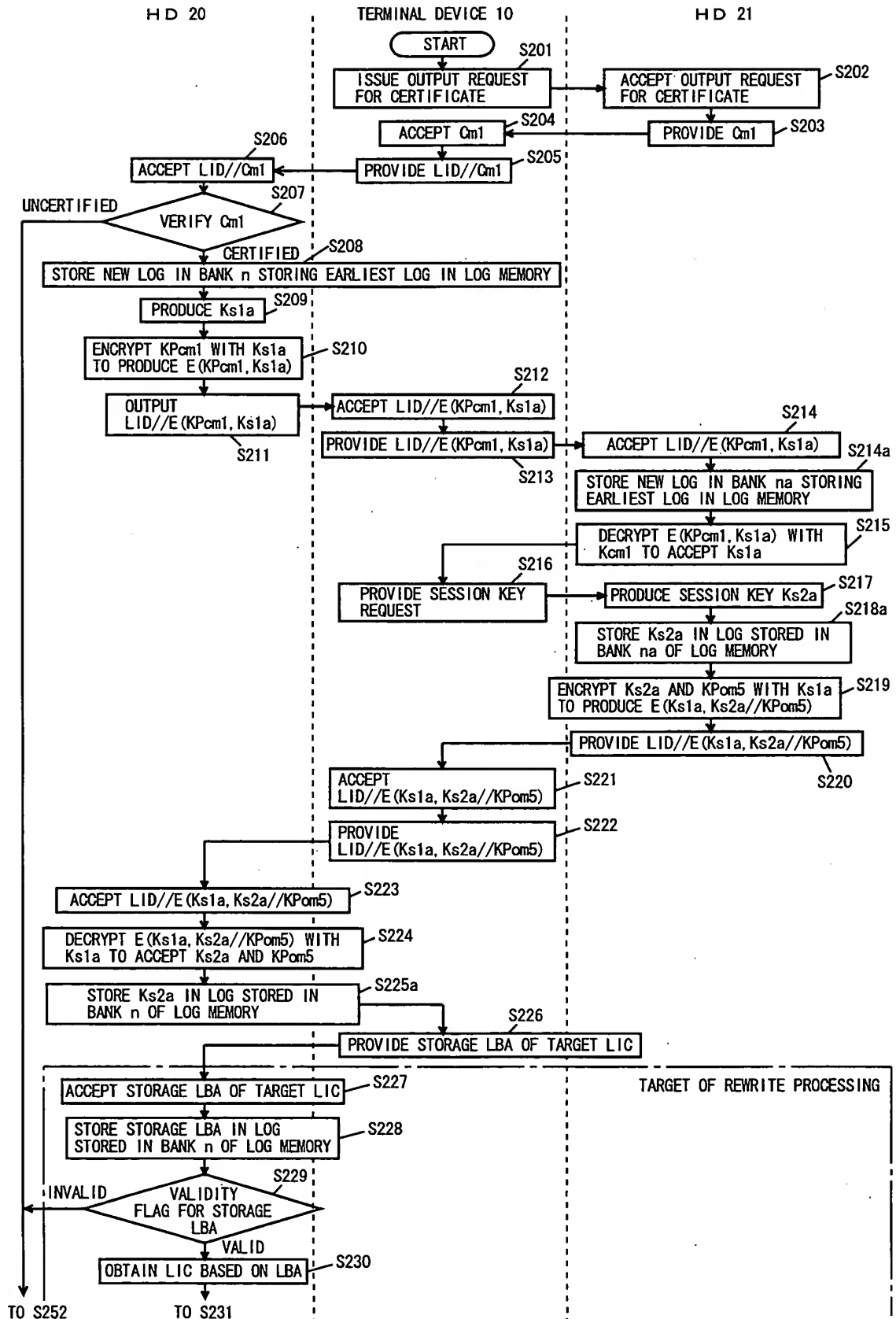


FIG. 27



Rec'd PET/PTO 24 JAN 2005

FIG. 28



```

graph TD
    subgraph "HD 20"
        S207[S207] --> S229[S229]
        S229 --> S231{S231  
LIDS MATCH}
        S231 -- MISMATCH --> S232{S232  
CHECK AC}
        S231 -- MATCH --> S232
        S232 -- PROHIBITED --> S233[ENCRYPT LIC WITH KPom5  
TO PRODUCE E(KPom5, LIC)]
        S232 -- MATCH --> S233
        S233 --> S234[ENCRYPT E(KPom5, LIC) WITH Ks2a  
TO PRODUCE E(Ks2a, E(KPom5, LIC))]
        S234 --> S235{S235  
CHECK AC}
        S235 -- COPY --> S236[CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO INVALID]
        S235 -- SHIFT --> S236
        S236 --> S237[CHANGE ST1 OF LOG STORED IN  
BANK n OF LOG MEMORY TO "SENT"]
        S237 --> S238[PROVIDE  
E(Ks2a, E(KPom5, LIC))]
        S238 --> S239[ACCEPT  
E(Ks2a, E(KPom5, LIC))]
        S239 --> S240[PROVIDE  
E(Ks2a, E(KPom5, LIC))]
        S240 --> S241[ACCEPT E(Ks2a, E(KPom5, LIC))]
        S241 --> S242[DECRYPT E(Ks2a, E(KPom5, LIC)) WITH  
Ks2a TO ACCEPT E(KPom5, LIC)]
        S242 --> S243[DECRYPT E(KPom5, LIC) WITH  
Kom5 TO ACCEPT LIC]
        S243 --> S244[ACCEPT STORAGE LBA]
        S244 --> S245[STORE STORAGE LBA IN LOG  
STORED IN BANK na OF LOG MEMORY]
        S245 --> S246{S246  
LIDS MATCH}
        S246 -- MATCH --> S247[ISSUE ERROR NOTIFICATION]
        S246 -- MISMATCH --> S248[STORE LIC IN STORAGE LBA]
        S247 --> S249[CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO VALID]
        S248 --> S249
        S249 --> S250[CHANGE ST1 OF LOG STORED IN BANK  
na OF LOG MEMORY TO "RECEIVED"]
        S250 --> S251[NORMAL END]
    end

    subgraph "TERMINAL DEVICE 10"
        S231 -- MISMATCH --> S252[ISSUE ERROR NOTIFICATION]
        S232 -- PROHIBITED --> S252
        S235 -- COPY --> S252
        S235 -- SHIFT --> S252
        S237 --> S253[ACCEPT ERROR NOTIFICATION]
        S239 --> S253
        S240 --> S253
        S241 --> S253
        S242 --> S253
        S243 --> S253
        S244 --> S253
        S245 --> S253
        S246 -- MATCH --> S253
        S246 -- MISMATCH --> S253
        S247 --> S253
        S248 --> S253
        S249 --> S253
        S250 --> S253
        S251 --> S253
        S252 --> S254[END DUE TO WRITE  
REJECTION]
        S253 --> S254
        S254 --> S255[NORMAL END]
    end

    S252 --> S256[TARGET OF REWRITE PROCESSING]
    S256 --> S207

```

```

graph TD
    subgraph "HD 20"
        S207[S207] --> S229[S229]
        S229 --> S231{S231  
LIDS MATCH}
        S231 -- MISMATCH --> S232{S232  
CHECK AC}
        S231 -- MATCH --> S232
        S232 -- PROHIBITED --> S233[ENCRYPT LIC WITH KPom5  
TO PRODUCE E(KPom5, LIC)]
        S232 -- MATCH --> S233
        S233 --> S234[ENCRYPT E(KPom5, LIC) WITH Ks2a  
TO PRODUCE E(Ks2a, E(KPom5, LIC))]
        S234 --> S235{S235  
CHECK AC}
        S235 -- COPY --> S236[CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO INVALID]
        S235 -- SHIFT --> S236
        S236 --> S237[CHANGE ST1 OF LOG STORED IN  
BANK n OF LOG MEMORY TO "SENT"]
        S237 --> S238[PROVIDE  
E(Ks2a, E(KPom5, LIC))]
        S238 --> S239[ACCEPT  
E(Ks2a, E(KPom5, LIC))]
        S239 --> S240[PROVIDE  
E(Ks2a, E(KPom5, LIC))]
        S240 --> S241[ACCEPT E(Ks2a, E(KPom5, LIC))]
        S241 --> S242[DECRYPT E(Ks2a, E(KPom5, LIC)) WITH  
Ks2a TO ACCEPT E(KPom5, LIC)]
        S242 --> S243[DECRYPT E(KPom5, LIC) WITH  
Kom5 TO ACCEPT LIC]
        S243 --> S244[ACCEPT STORAGE LBA]
        S244 --> S245[STORE STORAGE LBA IN LOG  
STORED IN BANK na OF LOG MEMORY]
        S245 --> S246{S246  
LIDS MATCH}
        S246 -- MATCH --> S247[ISSUE ERROR NOTIFICATION]
        S246 -- MISMATCH --> S248[STORE LIC IN STORAGE LBA]
        S247 --> S249[CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO VALID]
        S248 --> S249
        S249 --> S250[CHANGE ST1 OF LOG STORED IN BANK  
na OF LOG MEMORY TO "RECEIVED"]
        S250 --> S251[END]
    end

    subgraph "TERMINAL DEVICE 10"
        S231 -- MISMATCH --> S252[ISSUE ERROR NOTIFICATION]
        S232 -- PROHIBITED --> S252
        S235 -- COPY --> S252
        S235 -- SHIFT --> S252
        S237 --> S253[ACCEPT ERROR NOTIFICATION]
        S238 --> S253
        S239 --> S253
        S240 --> S253
        S241 --> S253
        S242 --> S253
        S243 --> S253
        S244 --> S253
        S245 --> S253
        S246 -- MATCH --> S253
        S246 -- MISMATCH --> S253
        S247 --> S253
        S248 --> S253
        S249 --> S253
        S250 --> S253
        S251 --> S253
        S252 --> S254[END DUE TO WRITE REJECTION]
        S253 --> S254
        S254 --> S255[NORMAL END]
    end

    S252 --> S256[TARGET OF REWRITE PROCESSING]
    S256 --> S207

```

FIG. 30

